과학기술정보통신부

KISA 한국인터넷진흥원

영세·중소기업 원격 보안점검 서비스

[내서버] 돌보미

내서버 돌보미 서비스란?

예산, 인력 등의 부족으로 보안위협에 대한 선제적 대응의 한계가 있는 영세·중소기업의 보안수준 향상과 보안 면역력 강화를 위하여 기업의 주요서버를 대상으로 보안점검을 무상으로 제공하는 서비스

주요 서버의 원격 보안점검

- 서버(Windows, Unix)의 계정관리, 파일 권한관리 등 보안설정 점검
- Apache Log4j, SMB 등 소프트웨어 취약점 유무 점검
- 웹쉘 등 침해사고 흔적 유무 점검

자가진단도구 제공

- 기업 자체 서버 보안점검 및 취약점 관리를 위한 자가진단도구 제공
- Windows, Unix 서버의 보안점검 도구
- 서버 별 보안점검 결과 통합관리

01.신청/접수

- 보호나라 홈페이지 접수
  - URL : www.boho.or.kr

02.신청서 검토

- 지원대상 기업 여부 검토
  (중소기업 확인증 등 확인)

03.사전협의

- 점검대상 선정
- 점검일정 및 점검방안 협의

04.보안점검

- 원격보안점검 진행
  (필요시 현장방문 점검)

05.개선지원

- 취약점 개선 지원
- 보안교육 제공

서비스 지원 대상 기업

중소기업기본법 제2조 제1항에 의거한 중소기업

모집 기간 및 규모

모집기간 : `22.04.01 ~ `22.11.30
모집규모 : 영세·중소기업 300개社

점검 대상

기업의 주요 서버
- WEB/WAS 서버, DB 서버 등

헬프 데스크

- 운영시간 : 평일 09:00 ~ 18:00
- 연 락 처 : 02-6715-2332, 02-6715-2333, servercheck@krcert.or.kr

중소기업 원격 보안점검(내서버돌보미)

▣ 내서버돌보미 서비스란?

서버 보안 관리에 예산 및 기술적으로 어려움을 겪는 영세·중소기업을 대상으로 보안 점검 서비스를 제공하여 날로 진화하는 랜섬웨어 등 사이버 공격에 적극적인 대응을 통해 기업의 보안 수준 향상과 보안 면역력 강화를 위하여 기업의 주요 서버를 대상으로 보안 점검을 무상으로 제공하는 서비스

1. 보안 위협 사항 점검을 위한 **점검 기준**

· 영세·중소기업 업무 특성 및 다양한 운영 환경(레거시 환경, 클라우드 등) 고려
· 정보시스템 서비스 형태에 따른 중요도 고려, 단계별 점검 기준 수립
· 정보시스템 서비스 역할(웹서버, DB 서버, AP 서버, 로그수집서버 등)별 특화 점검기준
· 침해 사고 여부 파악을 위한 침해 사고 유형별 점검 항목

< illustrative >

구분	Unix 점검 영역	항목수	Windows 점검 영역	항목수
CCE (Common Configuration Enumeration)	계정 관리	41개	계정 관리	56개
	파일 및 디렉터리 관리		보안 관리	
	서비스 관리		서비스 관리	
	패치 관리		로그 관리	
	웹 서비스 관리		패치 관리	
	-		웹서비스 관리	
CVE (Common Vulnerabilities and Exposures)	Log4j 취약점 점검	5개	Log4j 취약점 점검	6개
	Tomcat(Ghostcat) 취약점 점검		Tomcat(Ghostcat) 취약점 점검	
	Heartbleed 취약점 점검		DoS 취약점 점검	
	Shellshock 취약점 점검		SMB(CVE-2017-0143) 취약점 점검	
	libssh 인증우회 취약점		Bluekeep 점검	
	-		SMBGhost 취약점 점검	
침해사고 흔적	SUID, SGID, Sticky bit 점검	5개	의심스러운 프로세스 실행 목록	5개
	Rootkit 점검		악의적인 자동 실행 목록	
	랜섬웨어 의심 파일		악의적인 웹쉘 탐지	
	악의적인 웹쉘 탐지		랜섬웨어 의심 파일	
	Hosts 파일 변조		hosts 파일 변조	
합계	-	51개	-	67개

* CCE : Common Configuration Enumeration
다양한 환경에서 보안설정 취약점을 일괄적으로 식별하기 위한 표준

* CVE : Common Vulnerabilities and Exposures
공개적으로 알려진 컴퓨터 보안 결함 목록

2. 영세·중소기업의 취약점 통합 관리가 가능한 **자가진단도구** 제공
   · 주요 서버(Windows, Unix) 별 취약점 통합 및 이력 관리
   · 통합 관리 화면을 통한 해당 기업의 서버 취약점 일괄 관리

■ 수집도구	■ 분석도구
· 서버의 설정 및 현황 수집 · Windows, Unix 계열 점검	· 스크립트 결과 파일 분석 · 점검대상 및 결과 통합관리 · 시스템 설정 현황 확인 · 취약점 조치 방법 제공

3. **전문교육**을 통한 기업 담당자의 전문역량 제고 (온라인 교육)
   · 지속적인 정보 보안 동향 정보 및 최신 공격 정보 등에 대한 교육
   · 이론과 실습을 병행하여 체계적인 교육 진행